

# DECODING OF SCROLL CODES

GEORGE H. HITCHING AND TRYGVE JOHNSEN

**ABSTRACT.** We define and study a class of codes obtained from scrolls over curves of any genus over finite fields. These codes generalize Goppa codes in a natural way, and the orthogonal complements of these codes belong to the same class. We show how syndromes of error vectors correspond to certain vector bundle extensions, and how decoding is associated to finding destabilizing bundles.

## 1. INTRODUCTION

In [J], the second author interpreted the syndrome space for traditional Goppa codes  $C(D, G)$  for divisors  $D, G$  on an algebraic curve  $X$  as a projective space  $\mathbf{P} = \mathbf{P}Ext(H, \mathcal{O}_X)^*$  of isomorphism classes of line bundle extensions. It is well known that an extension of line bundles

$$0 \rightarrow \mathcal{O}_X \rightarrow W \rightarrow H \rightarrow 0$$

is classified by its cohomology class  $\delta(W) \in H^1(X, \text{Hom}(H, \mathcal{O}_X)) \cong Ext(H, \mathcal{O}_X)$ , the null element of  $Ext(H, \mathcal{O}_X)$  corresponding to the class of the trivial extension

$$0 \rightarrow \mathcal{O}_X \rightarrow \mathcal{O}_X \oplus H \rightarrow H \rightarrow 0.$$

The curve  $X$  is embedded in  $\mathbf{P}$  in the following way: If  $x \in X$ , then  $x$  corresponds to the class of an extension which is the kernel of the map

$$Ext(H, \mathcal{O}_X) \rightarrow Ext(H, \mathcal{O}_X(x)).$$

In that case the middle term  $E$  has a quotient bundle  $\mathcal{O}_X(x)$ . Moreover, in general, the class of an extension  $W$  is in the kernel of the map

$$Ext(H, \mathcal{O}_X) \rightarrow Ext(H, \mathcal{O}_X(A)),$$

for an effective divisor  $A$  if and only if it is contained in  $Span(A)$  (defined in a standard way) after embedding  $X$  in  $\mathbf{P}$  as described. In that case  $W$  has a quotient bundle  $\mathcal{O}_X(A)$ . In this way  $\mathbf{P}$  is stratified into secant strata of the embedded  $X$  according to the  $s$ -invariant of the middle terms  $W$  of the extensions appearing. The process of error location then corresponds, for given syndrome (= class of extension  $W$ ), to find the right divisor  $A'$  linearly equivalent to  $A$  such that  $\mathcal{O}_X(A)$  is a quotient bundle of the middle term  $W$ . It is interesting to observe that syndromes of errors which are designed-correctable (that is, the number of errors is at most  $\lfloor \frac{d-1}{2} \rfloor$ , where  $d$  is the designed minimum distance  $deg(D - G)$ ) are precisely the ones corresponding to unstable extensions. Recall that an extension is unstable if and only if  $s(W) = 2deg(A) - deg(W) < 0$  for a line bundle  $A$  of minimal degree such that  $\mathcal{O}_X(A)$  is a quotient bundle of the middle term  $W$ ; equivalently, if  $W$  contains a line subbundle of degree greater than  $\frac{1}{2}deg(W)$ . This viewpoint has been utilized and studied through a series of papers; see [BC], [Co1], [Co2].

---

1991 *Mathematics Subject Classification.* 14J28 (14H51).

*Key words and phrases.* curves, scrolls, principal parts, linear codes, decoding, vector bundle extensions.

In this paper we will replace the divisor or line bundle  $G$  on the curve  $X$  with a locally free sheaf  $\mathcal{E}$  (or vector bundle  $E$ ) of arbitrary positive rank  $r$  and apply a similar construction. This gives rise to a scroll  $\mathbf{P}E$  and various scroll codes, some of which have been studied in several papers. See [Ha], [L], and [Na]. We show how syndromes and decoding can be interpreted in terms of vector bundle extensions for a particular class of such codes.

Here is a summary of the article. Firstly, we recall some facts about scrolls and vector bundles which will be needed. In §3, we define “SAGS codes”, a type of evaluation code which generalizes Goppa’s SAG codes to scrolls. In particular, these have the property that their dual codes can again be interpreted as evaluation codes. In §4, we recall or prove some facts about the geometry of vector bundle extensions, and in §5 we apply this to decoding and error correction on SAGS codes. In the final section, we make brief remarks about the applicability of these results to scroll codes which are not necessarily evaluation codes.

An important tool is the use of bundle-valued principal parts to define the codes. We believe this makes transparent the connection between syndromes, bundles and geometry.

**Acknowledgements:** The first author is supported by the Deutsche Forschungsgemeinschaft Schwerpunktprogramm “Globale Methoden in der komplexen Geometrie”. He also thanks the University of Bergen for financial support and hospitality.

## 2. SCROLLS AND VECTOR BUNDLES

In this section we introduce the objects with which we will be working. Firstly, we fix some notation.

We denote vector bundles over the curve  $X$  with Roman letters  $E, W, \mathcal{O}_X, K_X$  etc. and their sheaves of sections with the corresponding script letters  $\mathcal{E}, \mathcal{W}, \mathcal{O}_X, \mathcal{K}_X$  etc. If  $V$  is a vector space, then  $\mathbf{P}V$  is the projective space of codimension one linear subspaces in  $V$ . Similarly, for a vector bundle  $E \rightarrow X$  we define  $\mathbf{P}E$  to be the scroll whose fiber at  $x \in X$  is the projective space of codimension one linear subspaces of  $E|_x$ . If  $\Upsilon$  is a line bundle over some variety  $Y$ , we write  $|\Upsilon|$  for the projective space  $\mathbf{P}H^0(Y, \Upsilon)$ . If  $|\Upsilon|$  is nonempty, we have a natural map  $Y \dashrightarrow |\Upsilon|$ .

If  $V$  is a vector space and  $g \in V^*$  a nonzero linear form, we denote  $\langle g \rangle$  the line in  $V^*$  spanned by  $g$ , and also the point in  $\mathbf{P}V$  defined by  $g$ . We also use this notation for points of projectivized vector bundles.

Any vector bundle  $E \rightarrow X$  gives rise to a short exact sequence of  $\mathcal{O}_X$ -modules

$$0 \rightarrow \mathcal{E} \rightarrow \underline{\text{Rat}}(E) \rightarrow \underline{\text{Prin}}(E) \rightarrow 0$$

where  $\underline{\text{Rat}}(E)$  is the sheaf of rational sections of  $E$  and  $\underline{\text{Prin}}(E)$  the sheaf of principal parts<sup>1</sup> with values in  $E$ . Taking global sections, we obtain

$$(1) \quad 0 \rightarrow H^0(X, E) \rightarrow \text{Rat}(E) \rightarrow \text{Prin}(E) \rightarrow H^1(X, E) \rightarrow 0.$$

We denote  $\bar{\alpha}$  the principal part of a global rational section  $\alpha$  of  $E$ , and we write  $[p]$  for the cohomology class of a principal part  $p \in \text{Prin}(E)$ . See for example [K] for further information.

**Definition 2.1.** *Let  $\mathcal{E}$  be a locally free sheaf of rank  $r \geq 1$  on a curve  $X$ , chosen in such a way that the linear system  $\Upsilon = \mathcal{O}_{\mathbf{P}E}(1)$  on the corresponding  $\mathbf{P}^{r-1}$ -bundle  $\mathbf{P}E$  over  $X$  is*

---

<sup>1</sup>Note that this is a different object from the “principal part sheaf”  $\mathcal{P}_X^k(\mathcal{E})$  considered by for example Laksov [L].

very ample, and  $h^1(\Upsilon) = 0$ . We map  $\mathbf{P}E$  into  $\mathbf{P}^{k-1}$  with the complete linear system  $H^0(\Upsilon)$ . The image  $T$  is by definition a smooth scroll, and isomorphic to  $\mathbf{P}E$ .

In particular, if  $X = \mathbf{P}^1$ , then  $\mathcal{E} = \mathcal{O}_{\mathbf{P}^1}(e_1) \oplus \cdots \oplus \mathcal{O}_{\mathbf{P}^1}(e_r)$ , with  $e_1 \geq \cdots \geq e_r \geq 1$  and  $\deg E = f = e_1 + \cdots + e_r \geq 2$ . In this case  $k = f + r$ , and the image  $T$  is by definition a rational normal scroll of type  $\mathbf{e} = (e_1, \dots, e_r)$ .

**Remark 2.2.** If the locally free sheaf  $\mathcal{E}$  satisfies certain stability conditions, then the dimension  $k$  is equal to  $\deg(\mathcal{E}) + r(1 - g)$  also for non-rational curves (twisting  $E$  with a large enough multiple of the line bundle corresponding to a fiber  $F$  if necessary). In general (see [Na], Proposition 2.1),

$$h^0(\mathcal{O}_{\mathbf{P}E}(b_1) \otimes \mathcal{O}_{\mathbf{P}E}(b_2 F)) = \binom{b_1 + r - 1}{r - 1} (\mu b_1 + b_2 + 1 - g)$$

in this case, where  $\mu(\mathcal{E})$  is the slope  $\frac{\deg \mathcal{E}}{r}$  of  $E$ . Here we only study the case  $b_1 = 1$ . From the proof of this result it also follows that  $h^1(X, E) = 0$  under these stability conditions, and this gives  $h^1(\mathbf{P}E, \Upsilon) = 0$ .

In the next section, we will describe some codes which can be produced from these objects.

### 3. MATRIX DESCRIPTION

In this section we will define a generalization of the strongly algebraic geometric (SAG) codes considered in [J].

**3.1. Strongly algebraic geometric scroll codes.** Let  $C$  be a code over a finite field  $\mathbb{F}_q$  defined as follows. Start with a scroll  $\mathbf{P}E$  over a curve  $X$ , which is embedded in  $\mathbf{P}^{k-1}$  as described above. Suppose  $\gamma$  is the number of  $\mathbb{F}_q$ -rational points on  $X$ ; if  $X = \mathbf{P}^1$  then  $\gamma = q + 1$ . Then we recall that  $T$  contains

$$(2) \quad n = \gamma(q^{r-1} + q^{r-2} + \cdots + q + 1)$$

points over  $\mathbb{F}_q$ . Choose  $s$  of the  $\gamma$  fibers of  $\mathbf{P}E$  over  $X$ , and in each fiber we pick at least  $r$  points, such that these points span the fiber. Altogether we have then chosen  $v$  points  $P_1, \dots, P_v$ , and  $sr \leq v \leq n$ . Let  $\Upsilon$  be the linear system on  $\mathbf{P}E$  described above, and look at the map  $\phi: H^0(\mathbf{P}E, \Upsilon) \rightarrow (\mathbb{F}_q)^v$  defined by  $\phi(f) = (f(P_1), \dots, f(P_v))$ . The code  $C$  is the image of  $\phi$ .

Let  $M$  be the divisor on  $\mathbf{P}E$  corresponding to the  $s$  fibers spanned by the  $P_i$ , so  $M$  is numerically (linearly if  $X = \mathbf{P}^1$ ) equivalent to  $sF$  on  $\mathbf{P}E$ , where  $F$  is the class of a fiber. Recall that  $\Upsilon$  is the bundle associated to the hyperplane system  $\mathcal{O}_{\mathbf{P}E}(1)$ . Look at the exact sequence of sheaves

$$0 \rightarrow \Upsilon(-M) \rightarrow \Upsilon \rightarrow \frac{\Upsilon}{\Upsilon(-M)} \rightarrow 0.$$

This induces an exact cohomology sequence

$$0 \rightarrow H^0(\Upsilon(-M)) \rightarrow H^0(\Upsilon) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow H^1(\Upsilon(-M)) \rightarrow H^1(\Upsilon) \rightarrow 0.$$

In turn this induces a sequence of maps

$$0 \rightarrow H^0(\Upsilon(-M)) \rightarrow H^0(\Upsilon) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow (\mathbb{F}_q)^v,$$

where each function on the union of the  $s$  chosen fibers is evaluated at the  $v$  points by the last map of the sequence. We denote this map by  $g$ . Of course we claim no exactness of the last sequence at  $(\mathbb{F}_q)^{sr}$ . We see from this that we can regard the linear code  $C$  as the image of the quotient space  $\frac{H^0(\Upsilon)}{H^0(\Upsilon(-M))}$ . In a special case considered by many authors one picks

all  $\mathbb{F}_q$ -rational points in all fibers, so  $s = \gamma$  and we pick  $q^{r-1} + \cdots + q + 1$  points in each fiber, and then  $v = n = \gamma(q^{r-1} + \cdots + q + 1)$ . The last two sequences above are simplified if  $H^0(\Upsilon(-M)) = 0$ . For  $X = \mathbf{P}^1$  this happens if  $s \geq e_1 + 1$ , and such an  $s$  can be chosen if  $q \geq e_1$ .

We now look at a special case:

Here we pick instead exactly  $r$  points in each of the  $s$  fibers, and we also pick them such that they span the fibers. Write  $D$  for the sum of the points of  $X$  over which the divisor  $M$  on  $\mathbf{P}E$  is supported. Clearly this is of the form  $x_1 + \cdots + x_s$  for distinct  $\mathbb{F}_q$ -rational points  $x_i \in X$ . For each  $i = 1, \dots, s$  we will denote the points in the fiber over  $x_i$  by  $P_{i,1}, \dots, P_{i,r}$ .

Then  $v = sr$ , the map  $g$  described above is an isomorphism of vector spaces, and we may identify the spaces  $(\mathbb{F}_q)^{sr}$  and  $(\mathbb{F}_q)^v$  of the last sequence, and regard the map  $H^0(\Upsilon) \rightarrow (\mathbb{F}_q)^{sr} = (\mathbb{F}_q)^v$  of the long exact cohomology sequence as an evaluation map in the  $v = sr$  points.

Now the cohomology  $H^0(\Upsilon)$  and  $H^1(\Upsilon(-M))$  can be identified with cohomology spaces of bundles on  $X$ . We have

$$H^0(\mathbf{P}E, \Upsilon) = H^0(X, E)$$

and

$$\begin{aligned} H^1(\mathbf{P}E, \Upsilon(-M)) &= H^1(X, E \otimes \pi_*(\mathcal{O}_{\mathbf{P}E}(-M))) \\ &= H^1(X, E \otimes \mathcal{O}(-D)) \\ &= H^0(X, K_X(D) \otimes E^*)^* \text{ by Serre duality} \\ &= H^0(\mathbf{P}E_1, \Upsilon_1)^* \end{aligned}$$

where  $\Upsilon_1$  is a suitable line bundle on a scroll  $\mathbf{P}E_1$ . Here  $E_1 = K_X(D) \otimes E^*$ , and  $\Upsilon_1$  is  $\mathcal{O}_{\mathbf{P}E_1}(1)$  for this locally free sheaf of rank  $r$  on  $X$ . We also get

$$H^1(T, \Upsilon) = H^1(X, \mathcal{E}) = H^0(X, K \otimes \mathcal{E}^*)^* = H^0(T_1, \Upsilon_1(-M))^*;$$

here and in the sequel, we denote by  $T_1$  the image of  $\mathbf{P}E_1$  by the linear system  $\mathcal{O}(1)$ . For  $X = \mathbf{P}^1$ , this becomes

$$\begin{aligned} H^1(\mathbf{P}E, \Upsilon(-sF)) &= H^1(\mathbf{P}^1, \mathcal{O}(e_1 - s) \oplus \mathcal{O}(e_2 - s) \oplus \cdots \oplus \mathcal{O}(e_r - s)) \\ &= H^0(\mathbf{P}^1, \mathcal{O}(s - e_1 - 2) \oplus \mathcal{O}(s - e_2 - 2) \oplus \cdots \oplus \mathcal{O}(s - e_r - 2))^* = H^0(T_1, \Upsilon_1)^*. \end{aligned}$$

In fact  $\Upsilon_1$  is  $\mathcal{O}(1)$  on  $\mathbf{P}E_1$ , where  $\mathcal{E}_1 = \mathcal{O}(s - e_d - 2) \oplus \mathcal{O}(s - e_{d-1} - 2) \oplus \cdots \oplus \mathcal{O}(s - e_1 - 2)$  on  $\mathbf{P}^1$ .

The identifications of the  $H^0$ -spaces follows from [Sc], p. 110. Moreover, this and the the identification of the  $H^1$ -spaces follows from a straightforward generalization of Lemma V, 2.4 of [H]: Clearly  $H^i(\Upsilon(-M))_x = H^i(\Upsilon_x) = 0$ , for all  $i > 0$  and all points  $x \in X$ , since  $\Upsilon|_x = \mathcal{O}_{\mathbf{P}^{d-1}}(1)$ . Therefore  $R^i(\pi_* \Upsilon(-M)) = 0$  for  $i > 0$ . See [H], Chapter III, Ex. 11.8., and Chapter III, Ex. 8.4.

We note that  $\mathbf{P}E_1 \cong \mathbf{P}E^*$ , since  $E_1 = E^* \otimes K_X(D)$ . Hence the long exact cohomology sequence becomes:

$$\begin{aligned} (3) \quad 0 \rightarrow H^0(\mathbf{P}E, \Upsilon(-M)) &\rightarrow H^0(\mathbf{P}E, \Upsilon) \rightarrow (\mathbb{F}_q)^{sr} \\ &\rightarrow H^0(\mathbf{P}E^*, \Upsilon_1)^* \rightarrow H^0(\mathbf{P}E^*, (\Upsilon_1 - M)^*) \rightarrow 0, \end{aligned}$$

which simplifies to

$$(4) \quad 0 \rightarrow H^0(\mathbf{P}E, \Upsilon) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1)^* \rightarrow 0$$

if  $h^0(\mathbf{P}E, \Upsilon(-M)) = h^1(\mathbf{P}E, \Upsilon) = 0$ . Dualizing, we get

$$(5) \quad 0 \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1(-M)) \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1) \rightarrow (\mathbb{F}_q)^v \\ \rightarrow H^0(\mathbf{P}E, \Upsilon)^* \rightarrow H^0(\mathbf{P}E, \Upsilon(-M))^* \rightarrow 0$$

which simplifies to

$$(6) \quad 0 \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow H^0(\mathbf{P}E, \Upsilon)^* \rightarrow 0$$

under the conditions stated. This motivates the following, generalizing the definition of a SAG code (see [J], §2).

**Definition 3.1.** *A scroll code  $C$  defined as above by evaluation of sections of  $\Upsilon$  at exactly  $r$  independent points of  $s$  fibers is called a strongly algebraic geometric scroll code or SAGS code if  $h^0(\mathbf{P}E, \Upsilon(-M)) = h^1(\mathbf{P}E, \Upsilon) = 0$ .*

The sequences (3) and (4) give that we obtain a generator matrix for  $C$  by evaluating sections in  $H^0(\mathbf{P}E, \Upsilon)$  at the  $v$  points. On the other hand, (5) and (6) show that we get a generator matrix for (a code equivalent to)  $C^*$ , that is, a parity check matrix for  $C$ , by evaluating sections in  $H^0(\mathbf{P}E^*, \Upsilon_1)$  at some  $v$  “dual” points (all of them in fibers corresponding to the same  $s$  points over  $\mathbf{P}^1$ ). We will say more about this in the next section.

**Remark 3.2.** Recall that a Goppa code  $C(D, G)$  is strongly algebraic geometric if  $2g - 2 < \deg G < s$ . In analogy with this, we notice that  $C$  is a SAGS code if  $E$  is semistable and the following inequality holds:

$$(7) \quad r(2g - 2) < \deg(E) < rs.$$

For example, suppose  $s \geq 2g$ . By [Na], Remark 2.1, there exist semistable (in fact, even so-called  $p$ -semistable) bundles of degree zero and rank  $r$  on  $X$  for  $X$ ,  $r$  and  $q$  “general enough”. Twisting such a bundle by an effective divisor of degree strictly between  $2g - 2$  and  $s$ , we get an  $E$  which defines a SAGS.

**3.2. Another description of the codes.** Here we give another way of defining the codes  $C$  and  $C^*$  which will be useful for our work later with extensions.

At each  $x \in X$ , a section  $t$  of  $\mathcal{O}_{\mathbf{P}E}(1) \rightarrow \mathbf{P}E$  restricts to a linear form  $t(x)$  on the projective space  $\mathbf{P}E|_x$ ; that is, a vector in  $E|_x$ . Evaluation of  $t$  at  $P = \langle e^* \rangle \in \mathbf{P}E|_x$  is simply restriction of  $t(x)$  to the line in  $E^*|_x$  spanned by  $e^*$ . The points  $P_{1,1}, \dots, P_{s,r}$  come from covectors  $e_{1,1}^*, \dots, e_{s,r}^* \in E^*$  which form a basis of each of the fibers of  $E^*$  over the points of  $D$ . Thus there exist unique  $e_{1,1}, \dots, e_{s,r} \in E$  such that  $e_{i,j}^*(e_{i',j'}) = \delta_{j,j'}$ , when this contraction makes sense (that is, when  $x_{i'} = x_i$ ). For each  $(i, j)$ , we have  $\langle e_{i,j}^* \rangle^* = \langle e_{i,j} \rangle$ , and restriction of  $t(x)$  to  $\langle e_{i,j}^* \rangle$  yields

$$(\text{coefficient of } e_{i,j} \text{ in } t(x_i)) \cdot e_{i,j}$$

which is well defined since the set of all the  $e_{i,j}$  includes a basis of each of the chosen fibers. We write  $\lambda_{i,j}$  for this coefficient. Identifying  $\mathbb{F}_q^{sr}$  with  $\bigoplus_{i,j} \mathbb{F}_q \cdot e_{i,j}$ , we see that  $t$  is sent to the  $sr$ -tuple  $(\lambda_{1,1}, \dots, \lambda_{s,r})$ . If we write this more suggestively as

$$((\lambda_{1,1}, \dots, \lambda_{1,r}), \dots, (\lambda_{s-1,1}, \dots, \lambda_{s,r}))$$

and consider  $t$  now as a section of the vector bundle  $E \rightarrow X$ , then we see that the  $r$ -tuple  $(\lambda_{i,1}, \dots, \lambda_{i,r})$  is just the expression of  $t(x_i)$  in terms of our chosen basis of  $E|_{x_i}$ . We have

natural identifications

$$E|_D = \bigoplus_{i,j} \mathbb{F}_q \cdot e_{i,j} = \bigoplus_{i,j} \mathcal{O}_{\mathbf{P}E}(1)|_{\langle e_{i,j}^* \rangle}$$

allowing us to pass between the interpretations of  $t$  as a section of  $E \rightarrow X$  and of  $\mathcal{O}_{\mathbf{P}E}(1) \rightarrow \mathbf{P}E$ . Thus the sequence (4) is identified with  $0 \rightarrow H^0(X, E) \rightarrow E|_D \rightarrow H^1(X, E(-D)) \rightarrow 0$ .

We now set  $H := E^*(D)$ . Note that  $H = \pi_*(\mathcal{O}_{\mathbf{P}E^*}(1) \otimes M)$ . Now  $E|_D = H^*(D)|_D$ , which can be viewed as (the global sections of) the subsheaf of  $\underline{\text{Prin}}(H^*)$  of principal parts supported at  $D$  with at most simple poles. For each  $(i, j)$ , let  $p_{i,j} \in \text{Prin}(H^*)$  be the principal part defined by  $e_{i,j}$ . (Of course, this is supported at  $x_i$  with a simple pole.) Then we have  $H^*(D)|_D = \bigoplus_{i,j} \mathbb{F}_q \cdot p_{i,j}$  and the sequence (4) becomes

$$0 \rightarrow H^0(X, H^*(D)) \xrightarrow{\rho} H^*(D)|_D \xrightarrow{\nu} H^1(X, H^*) \rightarrow 0$$

where  $\rho$  and  $\nu$  are induced by the principal part map<sup>2</sup> and the coboundary map in (1) respectively. Explicitly,  $\rho$  sends a rational section of  $H^*$  with poles bounded by  $D$  to its principal part, and  $\nu$  sends a principal part  $\lambda_{1,1}p_{1,1} + \dots + \lambda_{s,r}p_{s,r}$  to the cohomology class  $\left[ \sum_{i,j} \lambda_{i,j} p_{i,j} \right]$ .

Thus the code  $C$  is identified with the subspace of  $H^*(D)|_D$  of elements occurring as principal parts of global rational sections of  $H^*$ , and the syndrome of an element in  $\mathbb{F}_q^{sr}$  corresponds to the obstruction to lifting it to a global rational section of  $H^*$ .

**3.3. Generator and parity check matrices.**<sup>3</sup> In [J], generator and parity check matrices are given for the codes  $C$  and  $C^*$  when  $r = 1$ , that is,  $\mathbf{P}E$  is the curve  $X$ . Here we generalize this approach to the present situation.

Let  $t_1, \dots, t_l$  be a basis for  $H^0(X, E)$ . For each  $m = 1, \dots, l$  and each  $(i, j)$ , write  $\lambda_{m,(i,j)}$  for the coefficient of  $e_{i,j}$  in  $t_m(x_i)$ . Then by the last paragraph, the evaluation map sends  $t_m$  to the principal part  $\lambda_{m,(1,1)}p_{1,1} + \dots + \lambda_{m,(s,r)}p_{s,r}$ , so the matrix of  $\rho$  with respect to the bases  $\{t_m\}$  and  $\{p_{i,j}\}$  is

$$\begin{pmatrix} \lambda_{1,(1,1)} & \cdots & \lambda_{l,(1,1)} \\ \vdots & & \vdots \\ \lambda_{1,(s,r)} & \cdots & \lambda_{l,(s,r)} \end{pmatrix} =: S.$$

In order to find a matrix for  $\nu$ , in fact we will find one for  ${}^t\nu: H^1(X, H^*)^* \rightarrow (\mathbb{F}_q^{sr})^*$  and dualize. We recall explicitly the Serre duality pairing

$$H^0(X, K_X \otimes H) \times H^1(X, H^*) \rightarrow H^1(X, K_X) = \mathbb{F}_q.$$

Let  $p$  be an  $H^*$ -valued principal part and  $[p]$  its cohomology class; by (1), every class in  $H^1(X, H^*)$  is of this form. Let  $u$  be a global section of  $K_X \otimes H$ . Then  $u(p) \in \text{Prin}(K_X)$  and the contraction of  $u$  and  $[p]$  is simply  $[u(p)]$ . Hence  ${}^t\delta(u)$  is the linear form given by  $u \mapsto (p \mapsto [u(p)])$ .

Now, for each  $i$ , let  $z_i$  be a local coordinate on  $X$  centered at  $x_i$ . We fix an isomorphism  $\mathbb{F}_q \xrightarrow{\sim} H^1(X, K_X)$  and let  $c$  be the image of 1. We describe a basis of  $(\mathbb{F}_q^{sr})^*$  dual to the basis  $p_{(1,1)}, \dots, p_{(s,r)}$  of  $\mathbb{F}_q^{sr}$ . For each  $(i, j)$ , let  $h_{i,j} \in H$  be such that  $\langle h_{i,j} \rangle$  is the image of  $\langle e_{i,j}^* \rangle$  under the natural isomorphism  $\mathbf{P}E = \mathbf{P}(H^*(D)) \xrightarrow{\sim} \mathbf{P}H^*$ . We define a linear form

<sup>2</sup>Since the poles are all simple, we could also think of this as the sum of the residue maps over the points of  $D$ .

<sup>3</sup>This subsection is logically independent of the rest.

$\overline{h_{i,j}}$  on  $\mathbb{F}_q^{sr} = \bigoplus_{i,j} \mathbb{F}_q \cdot p_{i,j}$  by  $p \mapsto [dz_i \otimes h_{i,j}(p)]$ . By construction,  $\overline{h_{i,j}}(p_{i',j'})$  is nonzero if and only if  $j = j'$  and  $i = i'$ . Multiplying the  $h_{i,j}$  by nonzero scalars if necessary, we can assume that  $\overline{h_{i,j}}(p_{i',j'}) = c \cdot \delta_{i,i'} \delta_{j,j'}$ , so we obtain the required basis.

Now let  $u \in H^0(K_X \otimes H)$ . As we did for  $E$  and  $E^*$ , for each  $(i, j)$ , let  $h_{i,j}^*$  be the dual basis vector of  $h_{i,j}$  in  $H^*$ . (Up to nonzero scalar,  $h_{i,j}^* = e_{i,j} z_i$ .) Then

$$(8) \quad {}^t\delta(u)(p_{i,j}) = [p_{i,j}(u)] = \left[ \frac{u(x_i)(h_{i,j}^*)}{z_i} \right] = c \cdot (\text{coefficient of } dz_i \otimes h_{i,j} \text{ in } u(x_i))$$

Let us view  $u$  as a section of the line bundle  $\pi^* K_X \otimes \mathcal{O}_{\mathbf{P}H}(1)$ . To evaluate  $u$  at the point  $\langle h_{i,j}^* \rangle$ , we restrict  $u(x_i) \in (K_X \otimes H)|_{x_i}$  to the line  $\langle h_{i,j}^* \rangle$  in  $H^*|_{x_i}$ . This gives an element of  $K_X|_{x_i} \otimes \langle h_{i,j}^* \rangle^* = \mathbb{F}_q \cdot (dz_i \otimes h_{i,j})$ , and the coefficient is the same as that of  $c$  in (8).

Thus, if  $u(x_i) = dz_i \otimes (\mu_{i,1} h_{i,1} + \cdots \mu_{i,r} h_{i,r})$  for each  $i$ , then

$${}^t\nu(u) = \mu_{1,1} \overline{h_{1,1}} + \cdots \mu_{s,r} \overline{h_{s,r}}$$

is the expression of  ${}^t\nu(u)$  with respect to the basis  $\overline{h_{1,1}}, \dots, \overline{h_{s,r}}$ . Thus we can view  ${}^t\nu(u)$  as the evaluation of  $u$  at each of the points  $\langle h_{i,j}^* \rangle \in \mathbf{P}H$ , expressed in terms of the  $h_{i,j}$ .

Let now  $u_1, \dots, u_{l'}$  be a basis for  $H^0(X, K_X \otimes H)$ . For each  $n = 1, \dots, l'$ , write  $\mu_{n,(i,j)}$  for the coefficient of  $dz_i \otimes h_{i,j}$  in  $u_n(x_i)$ . Then the matrix of  ${}^t\nu$  with respect to our chosen bases is

$$\begin{pmatrix} \mu_{1,(1,1)} & \cdots & \mu_{l',(1,1)} \\ \vdots & & \vdots \\ \mu_{1,(s,r)} & \cdots & \mu_{l',(s,r)} \end{pmatrix} =: {}^tR.$$

The rows of this matrix give generators for  $C^*$ . But the  $(ri+j)$ th row represents the values of each of the  $u_n$  at  $\langle h_{i,j}^* \rangle$ , so we see explicitly how  $C^*$  is also an evaluation code. The matrix of  $\delta$  with respect to  $\{p_{1,1}, \dots, p_{s,r}\}$  and the basis of  $H^1(X, H^*)$  dual to  $\{u_1, \dots, u_{l'}\}$  is  $R$ . By exactness,  $RS = 0$  and  ${}^tS^tR$  are zero, and  ${}^tS$  and  $R$  are parity check matrices for  $C^*$  and  $C$  respectively.

**Note:** As we have defined them,  $C$  and  $C^*$  belong to different vector spaces. However, since we have the mutually dual bases  $\{p_{i,j}\}$  and  $\{\overline{h_{i,j}}\}$ , we can view both codes as subspaces of  $\mathbb{F}_q^{rs}$  via the vector space isomorphism  $\mathbb{F}_q^{rs} \xrightarrow{\sim} (\mathbb{F}_q^{rs})^*$  sending each  $\overline{h_{i,j}}$  to  $p_{i,j}$ .

**Remark 3.3.** It follows from the discussion above that the orthogonal complements (or duals) of SAGS codes are (code equivalent to) SAGS codes in general, just like for the traditional case  $r = 1$ . Hence the description above lends itself just as well to make parity check matrices as to make generator matrices. This is one of the virtues of Goppa codes (based on curves), which it has been hard to reproduce for codes produced from varieties of higher dimension. If one picks all points of for example Grassmannians or scrolls, then the coordinates of these points are suitable for producing columns of generator matrices of codes that are interesting. But if one tries to use the same points as columns of parity check matrices, then because of the existence of linear spaces inside the varieties (lines), one cannot exceed minimum distance 3. Hence, in order to get essentially self-dual classes of codes, like for Goppa codes, one must revise the way one picks points.

**3.4. The link with extensions.** Since the column vectors of the parity check matrix of  $C$  are described through coordinates of points of  $\mathbf{P}E^*$  embedded by the complete linear system  $\Upsilon_1$ , we see that the (projectivized) syndrome space of  $C$  in a natural way is identified with

$$\mathbf{P}H^0(\mathbf{P}E^*, \Upsilon_1) = \mathbf{P}H^0(X, K(D) \otimes E^*).$$

If  $X = \mathbf{P}^1$  and  $\Upsilon = \mathcal{O}(e_1) \oplus \cdots \mathcal{O}(e_d)$ , then this is

$$\mathbf{P}H^0(\mathbf{P}E^*, \Upsilon_1) = \mathbf{P}H^0(\mathbf{P}^1, \mathcal{O}(s - e_1 - 2) \oplus \mathcal{O}(s - e_2 - 2) \oplus \cdots \oplus \mathcal{O}(s - e_d - 2))$$

The syndrome space can also be identified with

$$H^1(X, E \otimes M^*) = H^1(X, H^*),$$

where as before  $H^* = E(-D)$ . For  $X = \mathbf{P}^1$  and  $\Upsilon = \mathcal{O}(e_1) \oplus \cdots \mathcal{O}(e_d)$ , this is

$$H^1(\mathbf{P}^1, \mathcal{O}(e_1 - s)) \oplus \mathcal{O}(e_2 - s)) \oplus \cdots \oplus \mathcal{O}(e_d - s)) = H^1(X, H^*),$$

where  $H = \mathcal{O}(s - e_1) \oplus \mathcal{O}(s - e_2) \oplus \cdots \oplus \mathcal{O}(s - e_d)$ .

Now  $H^1(X, H^*) = \text{Ext}^1(\mathcal{O}_X, H^*)$  can be identified with isomorphism classes of extensions

$$0 \rightarrow H^* \rightarrow W \rightarrow \mathcal{O}_X \rightarrow 0.$$

In the next section, we will relate the geometry of the space  $\mathbf{P}H^1(X, H^*)^*$  to the behaviour of these extensions.

#### 4. GEOMETRY OF EXTENSION SPACES

Henceforth, to allow for slightly greater generality, instead of the bundle  $H^*$  we will work with  $\text{Hom}(F_2, F_1)$  for bundles  $F_1$  and  $F_2$  over  $X$ . Recall that the *decomposable locus* of  $\text{Hom}(F_2, F_1)$  is the locus of maps of rank one. This is a determinantal subvariety of  $\text{Hom}(F_2, F_1)$ , defined by the vanishing of all  $2 \times 2$  minors of the maps. We denote  $\Delta$  the locus defined by these (homogeneous) polynomials in  $\mathbf{P}\text{Hom}(F_2, F_1)^*$ .

**Example 4.1.** If  $F_1$  and  $F_2$  are both of rank two then  $\Delta$  is a bundle of smooth quadrics in the  $\mathbf{P}^3$ -bundle  $\mathbf{P}\text{Hom}(F_2, F_1)^* \rightarrow X$ . Of course, if either one is a line bundle then  $\Delta = \mathbf{P}\text{Hom}(F_2, F_1)^*$ .

**4.1. Embeddings of scrolls.** Here we give another description of the map from  $\mathbf{P}H$  into the projectivized syndrome space  $\mathbf{P}H^1(X, H^*)^*$ , which will be adapted for our study of extensions.

Let  $V \rightarrow X$  be any vector bundle. We have a short exact sequence

$$0 \rightarrow \mathcal{V} \rightarrow \mathcal{V}(x) \rightarrow \frac{\mathcal{V}(x)}{\mathcal{V}} \rightarrow 0$$

whose cohomology sequence includes

$$\cdots \rightarrow H^0(X, V(x)) \rightarrow V(x)|_x \rightarrow H^1(X, V) \rightarrow \cdots$$

Since  $\mathbf{P}(V^*(-x))|_x$  is canonically isomorphic to  $\mathbf{P}V^*|_x$ , the projectivized coboundary map gives rise to a map  $\psi_x: \mathbf{P}V^*|_x \dashrightarrow \mathbf{P}H^1(X, V)^*$ . We define a map  $\psi: \mathbf{P}V^* \dashrightarrow \mathbf{P}H^1(X, V)^*$  by taking the product of all the  $\psi_x$ .

Now by Serre duality and the projection formula, we have an identification

$$(9) \quad H^1(X, V) \xrightarrow{\sim} H^0(\mathbf{P}V^*, \pi^*K_X \otimes \mathcal{O}_{\mathbf{P}V^*}(1))^*.$$

**Lemma 4.2.** ([Hi], §2) *Via the above identification,  $\psi$  coincides with the standard map  $\mathbf{P}V^* \dashrightarrow |\pi^*K_X \otimes \mathcal{O}_{\mathbf{P}V^*}(1)|$ . Moreover,  $\psi$  is an embedding if and only if for all  $x, y \in X$ , we have  $h^0(X, K_X(-x - y) \otimes V^*) = h^0(X, K_X \otimes V^*) - 2r$ .*

**Remark 4.3.** The key feature of this interpretation is that  $\psi$  sends  $\langle v \rangle \in \mathbf{P}V^*|_x$  to the projectivized cohomology class of a  $V$ -valued principal part supported at  $x$  with a simple pole in the direction  $v$ . This will allow us to use the alternative construction of the code  $C$  in §3.2 to understand the geometry of the syndromes.



We recall a definition:

**Definition 4.4.** *Let  $F_2 \rightarrow X$  be a vector bundle. Then an elementary transformation of  $F_2$  is a vector bundle defined by a locally free subsheaf of  $\mathcal{F}_2$  of rank equal to the rank of  $F_2$ .*

Such subsheaves can be defined using principal parts. If  $F_1$  is another vector bundle over  $X$ , then any  $\text{Hom}(F_2, F_1)$ -valued principal part naturally defines a map  $\mathcal{F}_2 \rightarrow \underline{\text{Prin}}(F_1)$ . Then the kernel of such a map defines an elementary transformation of  $F_2$ . Moreover, any elementary transformation of  $F_2$  is of this form (although not in a unique way).

We will need the following technical result on extension classes:

**Lemma 4.5.** ([Hi], §4.1) *Let  $W$  be an extension of  $F_2$  by  $F_1$ . An elementary transformation of  $\mathcal{G}$  of  $\mathcal{F}_2$  lifts to a vector subbundle of  $W$  if and only if the class  $\delta(W)$  of the extension can be defined (cf. (1)) by a principal part  $p \in \text{Prin}(\text{Hom}(F_2, F_1))$  such that  $\mathcal{G} = \text{Ker}(p: \mathcal{F}_2 \rightarrow \underline{\text{Prin}}(F_1))$ .*

Now we can give the main result of this section.

**Theorem 4.6.** *Let  $0 \rightarrow F_1 \rightarrow W \rightarrow F_2 \rightarrow 0$  be a nontrivial extension. Then  $\langle \delta(W) \rangle$  belongs to the linear span of at most  $h$  independent points of  $\Delta|_D$  if and only if  $W$  has a subbundle lifting from an elementary transformation of  $F_2$  of the form*

$$(10) \quad 0 \rightarrow \mathcal{G} \rightarrow \mathcal{F}_2 \rightarrow \tau \rightarrow 0$$

where  $\tau \subset \underline{\text{Prin}}(F_1)$  is a skyscraper sheaf of length at most  $h$  supported on  $D$  and with at most simple poles.

*Proof.* Suppose  $\langle \delta(W) \rangle$  belongs to the linear span of at most  $h$  independent points of  $\Delta|_D$  in  $\mathbf{P}H^1(X, H^*)^*$ . Then by the alternative definition of  $\psi$  given above,  $\delta(W)$  can be defined by  $p \in \text{Prin}(\text{Hom}(F_2, F_1))$  of the form  $\sum_{j=1}^h p_j$  where each  $p_j$  is a principal part supported at one point of  $D$  with a simple pole along some rank one map. Thus we have a short exact sequence

$$0 \rightarrow \mathcal{G} \rightarrow \mathcal{F}_2 \xrightarrow{p} \tau \rightarrow 0$$

where  $\tau \subset \underline{\text{Prin}}(F_1)$  is a skyscraper sheaf of length at most  $h$  supported on  $D$  and with at worst simple poles. By Lemma 4.5, the sheaf  $\mathcal{G}$  lifts to a subbundle of  $W$ .

Conversely, suppose an elementary transformation  $\mathcal{G}$  of  $\mathcal{F}_2$  of the stated type lifts to a subbundle of  $W$ . By Lemma 4.5, the class  $\delta(W)$  can be defined by some  $p \in \text{Prin}(\text{Hom}(F_2, F_1))$  which, viewed as a map  $\mathcal{F}_2 \rightarrow \underline{\text{Prin}}(F_1)$ , has kernel  $\mathcal{G}$ . From the sequence (10) we deduce that  $p$  is supported along  $D$  and has at most simple poles. We write  $p = \sum_{x \in D} p_x$ , where each  $p_x$  is a principal part supported at one point  $x$ , and then write each  $p_x$  as a sum of rank one homomorphisms, of minimal length. Since  $\tau$  is of length at most  $h$ , any such expression for  $p$  contains at most  $h$  independent such rank one homomorphisms. By the alternative definition of  $\psi$ , the point  $\langle \delta(W) \rangle$  is contained in the span of these at most  $h$  rank one points of  $\text{Hom}(F_2, F_1)$ .  $\square$

**Remark 4.7.** Suppose  $F_1 = H^*$  and  $F_2 = \mathcal{O}_X$ , so we are in the situation of the last section. Then this theorem shows that the extension  $0 \rightarrow H^* \rightarrow W \rightarrow \mathcal{O}_X \rightarrow 0$  can be “quasi-inverted” to a short exact sequence

$$0 \rightarrow \mathcal{O}_X(-A) \rightarrow W \rightarrow (H^*)' \rightarrow 0$$

for some effective divisor  $A \leq D$  and some bundle  $(H^*)'$ , if and only if  $\langle \delta(W) \rangle$  lies in the linear span of some points of  $\mathbf{P}H^*$  all lying over the support of the divisor  $A \leq D$ . In this case the rank of each  $\phi_x$  can be at most 1.

**Remark 4.8.** When  $\mathbb{F}_q$  is replaced with the complex number field, a generalization of Theorem 4.6 is proven in [Hi], Theorem 4. For example,  $p$  may have poles of higher order. However, the above proof suffices for the situation we are considering.

Now we give some alternative ways of viewing the condition of Theorem 4.6. Firstly, it is equivalent to saying that  $\delta(W)$  belongs to

$$\begin{aligned} \text{Ker}(H^1(X, \text{Hom}(\mathcal{O}_X, H^*)) &\rightarrow H^1(X, \text{Hom}(\mathcal{O}_X(-A), H^*))) \\ &= \text{Ker}(H^1(X, H^*) \rightarrow H^1(X, H^*(A))) \\ &= \text{Ker}(H^0(X, H(K))^* \rightarrow H^0(X, H(K-A))^*). \end{aligned}$$

We look instead at the (isomorphic) space of extensions of type

$$0 \rightarrow \mathcal{O}_X \rightarrow W \rightarrow H \rightarrow 0.$$

Then it follows from a dual version, as in [NR], Lemma 3.2, that there is a surjection  $W \rightarrow \mathcal{O}_X(A) \rightarrow 0$  if and only if  $\delta(W)$  belongs to

$$\begin{aligned} \text{Ker}(H^1(X, \text{Hom}(H, \mathcal{O}_X) \rightarrow H^1(X, \text{Hom}(H, \mathcal{O}_X(A)))) \\ = \text{Ker}(H^1(X, H^*) \rightarrow H^1(X, H^*(A))). \end{aligned}$$

We see that the two kernels are the same, and we have two alternative descriptions.

In the first description we may view  $\mathcal{O}_X(-A)$  as a special case of a locally free sheaf  $G$  with a sheaf injection  $\phi: G \rightarrow \mathcal{O}_X$ , such that  $\phi$  factors via a map  $G \rightarrow W$ .

In the second description  $\mathcal{O}_X(A)$  is a special case of a locally free sheaf  $G$  with a sheaf homomorphism  $\phi: \mathcal{O}_X \rightarrow G$ , such that  $\phi$  extends to a homomorphism  $W \rightarrow G$ .

The common kernel can also be viewed as that of a map

$$\text{Ext}(\mathcal{O}_X, H^*) \rightarrow \text{Ext}(\mathcal{O}_X, H^*(A)),$$

using Proposition 6.3 of [H]. Using Proposition 6.7 of [H], we interpret this as the kernel of a map

$$\text{Ext}(H, \mathcal{O}_X) \rightarrow \text{Ext}(H(-A), \mathcal{O}_X) = \text{Ext}(H, \mathcal{O}_X(A)).$$

**Example 4.9.** An easy case to handle is when  $X = \mathbf{P}^1$  and we pick all  $r$  points in each fiber along the directrix curves. Assume  $s = q + 1$ . It is clear that the natural subscroll of type  $(e_2, \dots, e_r)$  is contained in a hyperplane, and that any hyperplane containing this subscroll intersects the first directrix in  $e_1$  points, and for some such hyperplane they can be taken to be rational. One easily sees that this hyperplane contains  $e_1 + (r-1)(q+1)$  points, which is largest possible, and that the minimum distance of the code then is  $q + 1 - e_1$ . Working dually, with the scroll  $T_1$  of type  $(q-1-e_r, \dots, q-1-e_1)$ , we see that we get a linear dependency between  $q + 1 - e_1$  points on the directrix curve of smallest degree  $(q-1-e_1)$ , which again indicates minimum distance  $q + 1 - e_1$ . Furthermore the higher weights  $d_i$  increase by one until we reach a value of  $i$  such that no codimension  $i$ -space contains the subscroll of  $(e_2, \dots, e_r)$ . This space contains  $e_1 + e_2 + (r-2)(q+1)$  points, so  $d_i = 2q + 2 - e_1 - e_2$ . We leave it to the reader to make the remaining calculations to determine the complete weight hierarchy. It is a sad fact that a code with such a nice description has such bad code-theoretical properties.

## 5. ERROR CORRECTION

We return to the code  $C$ . Here we give a geometric condition for the correctability of the error, in terms of the image of the embedding of  $\mathbf{P} \operatorname{Hom}(F_2, F_1)^*$  in the syndrome space.

**Important hypothesis:** We will assume that the  $\operatorname{Hom}(F_2, F_1)$ -valued principal parts  $p_{1,1}, \dots, p_{s,r}$  are all along directions corresponding to rank one homomorphisms. This is possible since each fiber is spanned by such maps.

**5.1. A geometric condition for correctability.** The following is analogous to [J], Theorem 3.4.

**Theorem 5.1.** *Suppose a codeword  $\mathbf{x} \in C$  is transmitted, and  $\mathbf{y} = \mathbf{x} + \mathbf{e}$  is received. Let  $W$  be the extension of  $F_2$  by  $F_1$  defined by the syndrome class  $\nu(\mathbf{y}) = \nu(\mathbf{e})$ . Then the error  $\mathbf{e}$  has weight at most  $h$  only if  $W$  has a subbundle, necessarily of degree at least  $\deg(F_2) - h$ , lifting from an elementary transformation of  $F$  of the form*

$$0 \rightarrow \mathcal{G} \rightarrow \mathcal{F}_2 \rightarrow \tau \rightarrow 0$$

where  $\tau \subset \operatorname{Prin}(F_1)$  is a skyscraper sheaf of length at most  $h$  supported on  $D$  and with at most simple poles.

*Proof.* Suppose  $\mathbf{e}$  has weight  $h$ . Then  $\mathbf{e}$  is a principal part of the form

$$\lambda_{i_1, j_1} p_{i_1, j_1} + \dots + \lambda_{i_h, j_h} p_{i_h, j_h}$$

for some nonzero  $\lambda_{i_1, j_1}, \dots, \lambda_{i_h, j_h} \in \mathbb{F}_q$ , with the  $(i_h, j_h)$  all distinct. Then by Lemma 4.5, the kernel of the map of  $\mathcal{O}_X$ -modules  $\mathbf{e}: \mathcal{F}_2 \rightarrow \operatorname{Prin}(F_1)$  lifts to a subbundle of  $W$ . Since  $\mathbf{e}$  is supported along  $D$  and is a sum of  $h$  rank one elements of  $\operatorname{Hom}(F_2, F_1)$  with at most simple poles along  $D$ , this subbundle is an elementary transformation of the stated type.  $\square$

**Remark 5.2.** As in Theorem 3.4 of [J], we can give a geometric interpretation of this situation. By Theorem 4.6, there are at most  $h$  errors in  $\mathbf{y}$  only if the class  $\langle \nu(\mathbf{e}) \rangle$  belongs to an  $h$ -secant plane to  $\Delta|_D$  spanned by at most  $h$  distinct points. Moreover, also as in [J], both the errors and the points of the scroll  $\mathbf{P}H^*$  are defined over  $\mathbb{F}_q$ .

**5.2. Error location.** Assume we have a code  $C$  as described above, and that we have picked exactly  $r$  points in each of  $s$  fibers, where  $s$  typically is the number of all  $\mathbb{F}_q$ -rational points on  $X$ . Assume a codeword is sent, and the syndrome calculated. If this is zero, there is no problem. Otherwise, look at the corresponding point in the projectivized syndrome space  $\mathbf{P} \operatorname{Ext}^1(\mathcal{O}_X, H^*)^* = \mathbf{P} \operatorname{Ext}^1(H, \mathcal{O}_X)^*$ . This is the space where the scroll  $\mathbf{P}H \cong \mathbf{P}E^* \cong T_1$  is embedded.

Now we think of error location in two steps. In Step 1 we find the various fibers of  $T_1$  such that the syndrome is a linear combination of points of these fibers. In Step 2 we find the individual points in these fibers such that the syndrome contribution from each given fiber is a linear combination of syndromes from these individual points. It is only in Step 1 that we can use the direct analogue with the situation studied in [BC], [Co1], [Co2] and [J]. On the other hand, Step 2 is basically only a linear algebra problem: the syndrome component from this fiber is a point of this fiber. Find which linear combination it is, of the  $r$  (dual) points that we have picked in this fiber in the first place.

Hence we focus on Step 1. View the syndrome as an extension

$$0 \rightarrow \mathcal{O}_X \rightarrow W \rightarrow H \rightarrow 0.$$

Error location is then to find the (hopefully) unique line bundle  $\mathcal{O}_X(A)$  of lowest degree such that there is a surjection of  $W$  onto  $\mathcal{O}_X(A)$ . Having found the divisor class, one must

find the effective divisor  $A'$  in the class such that the syndrome is spanned by the fibers of  $T_1$  corresponding to points on the divisor  $A'$ . This part of the process is described in Chapter 4 of [BC] for  $r = 1$ .

**Definition 5.3.** *For a rank  $r$  bundle  $V$  on a curve  $X$  we set  $s_1(V) = \deg V - r \max\{\deg L\}$ , for  $L$  a line subbundle of  $V$  on  $X$ .*

Then we have:

**Proposition 5.4.** *For a given syndrome point  $\nu(\mathbf{y})$ , interpreted as an extension of type*

$$0 \rightarrow H^* \rightarrow W \rightarrow \mathcal{O}_X \rightarrow 0,$$

*we have*

$$s_1(W) \leq (r+1)a - rs + \deg \mathcal{E},$$

*where  $a$  is the number of different fibers of  $T$  (over  $X$ ) we must use to pick points such that errors in the positions corresponding to these points give rise to the syndrome.*

*Proof.* If we use points from  $a$  different fibers to span the syndrome, where these fibers correspond to the points  $x_{i_1}, \dots, x_{i_a}$  on the curve, then  $\mathcal{A}^*$  is a subsheaf of rank one of  $\mathcal{W}$ , and

$$s_1(W) \leq \deg W + \deg A = \deg H^* + (r+1)a = \deg \mathcal{E} - rs + (r+1)a.$$

□

**Remark 5.5.** For  $r = 1$  and Goppa codes this gives  $s(W) \leq 2a - \deg(D - G) = 2a - d$ , where  $d$  is the designed minimum distance, and we see that if the number of errors is less than designed-correctable, then  $W$  is unstable.

What does it take to ensure that the fibers spanning a point can be uniquely chosen? Assume there are errors in two fibers. If the syndrome point  $\langle \nu(\mathbf{e}) \rangle$  is also in the span of two other fibers, then the span of the first two fibers has a common point with the span of the second group of two fibers, and the span of all four fibers is less than the “expected” value which is  $4r - 1$ . Hence a sufficient condition for this not to happen is

$$h^0(T_1, \Upsilon_1(-F_1 - F_2 - F_3 - F_4)) = h^0(X, E_1(-x_1 - x_2 - x_3 - x_4)) = h^0(X, E_1) - 4r$$

for all choices of  $x_1, x_2, x_3, x_4$ .

In general, syndromes from  $a$  fibers can be uniquely traced back to  $a$  fibers if

$$h^0(X, E_1(-B)) = h^0(X, E_1) - 2ar$$

for all choices of effective divisors  $B$  of degree  $2a$  (compare with Lemma 4.2).

For  $X = \mathbf{P}^1$  this happens if  $s - e_1 - 2 - 2a \geq -1$ . For curves of higher genus we have:

**Proposition 5.6.** *Let  $E$  be a stable bundle of rank  $r$  on  $X$ . Then errors in*

$$a < \frac{\mu(H)}{2} = \frac{s - \mu(\mathcal{E})}{2} = \frac{rs - \deg \mathcal{E}}{2r}$$

*different fibers can be traced back to a unique choice of  $a$  fibers.*

*Proof.* By Riemann–Roch, we have

$$h^0(X, E_1(-B)) = \deg E_1 - 2ra + r(1 - g) + h^0(K_X(B) \otimes E_1^*).$$

We show that  $h^0(X, K_X(B) \otimes E_1^*) = h^0(X, H^*(B)) = 0$ . Since  $E$  is stable, so is  $H^*$ , and one obtains  $h^0(X, H^*(B)) = 0$  unless  $2a \geq \mu(H)$ . (By the same argument,  $H^0(X, E_1) = \deg E_1 + r(1 - g)$ , so we obtain the desired conclusion.) □

**Remark 5.7.** Since one can correct errors from  $a$  fibers if  $a \leq \frac{\mu(H)-1}{2}$ , it is tempting to conclude that one can correct up to  $t = r \left( \frac{\mu(H)-1}{2} \right) = \frac{\deg H - r}{2}$  errors (which holds for  $r = 1$ , where  $\deg H$  is the designed minimum distance), since there are  $r$  points in each fiber. But the discussions so far only makes this true for  $t$  errors if they are clustered in as few as  $\frac{\mu(H)-1}{2}$  fibers. If they are “spread out” on more fibers, the discussion above does not ensure unique decoding of more than  $\frac{\mu(H)-1}{2}$  errors.

**Proposition 5.8.** *Suppose  $E$  is a stable bundle on  $X$ . Then the syndrome of an error which can be traced uniquely back to a choice of  $a$  fibers in the sense of the previous result, that is, where the number  $a$  of fibers where errors are made is at most  $\frac{\mu(H)}{2}$ , defines an extension  $0 \rightarrow H^* \rightarrow W \rightarrow \mathcal{O}_X \rightarrow 0$  with*

$$s_1(W) < \frac{(r-1)(\deg \mathcal{E} - sr)}{2r}.$$

*Proof.* Insert  $a = \frac{\mu(H)}{2} = \frac{rs - \deg \mathcal{E}}{2r}$  in the statement of Proposition 5.4.  $\square$

We see that the right hand side is strictly negative if  $r > 1$  and  $C$  is a SAGS code.

**Remark 5.9.** What can be said about the code parameters of the SAGS codes? Certainly the word length is  $sr$ . If enough fibers are chosen ( $s$  big enough) that the chosen fibers span the projective space  $\mathbb{P}^{k-1}$  in which  $T$  lies, then the dimension of the code is  $k$ . It is much harder to find the true minimum distance of the codes. All we can say is that it depends on the choice of the points in each fiber. The case studied in Example 4.9 obviously represents bad choices. To illustrate the problem of choosing points conveniently, look at the simplest case of a code which is not a Goppa code. We choose  $X = \mathbf{P}^1$ , and  $L = \mathcal{O}(1) \oplus \mathcal{O}(1)$ . Hence  $T$  is a quadric in  $X = \mathbf{P}^3$ . How can we choose 2 points on each line on one of the two families, such that as few as possible among the  $2q+2$  points are contained in the same plane. The worst case involves  $q+2$  points in a plane (take two lines  $L_1$  and  $L_2$  on the quadric, meeting in a point  $P$ ), and choose all  $q+1$  points on  $L_2$ , one additional point on  $L_1$ , and  $q$  additional points on lines parallel to  $L_1$ ). But there clearly exist better choices, unless  $q$  is very small. In general, the minimum distance guaranteed by the method, is  $s - 2 - e_1$  for codes from rational curves (Example 4.9) and  $\mu(H)$  for codes from curves of higher genus if  $E$  is stable (Proposition 5.6). But one can hope for much better true values with good choices of points.

**Remark 5.10.** The considerations above involve no direct decoding algorithm. Neither did [J]. Nevertheless the principles from [J] were used to approach concrete decoding in the series of papers [BC], [Co1], [Co2]. We feel that the generalization presented in the present paper of the line of thoughts in [J], should lend itself to a corresponding generalization of the results of these other papers.

## 6. SYNDROME DECODING OF OTHER CODES

Throughout this work we have insisted on picking exactly  $r$  points in each fiber when defining the codes. This is because we have defined the codes as evaluation codes, thus starting with a natural generator, and not a parity check matrix. To obtain the exact sequence

$$0 \rightarrow H^0(\mathbf{P}E, \Upsilon) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1)^* \rightarrow 0$$

and its dual counterpart

$$0 \rightarrow H^0(\mathbf{P}E^*, \Upsilon_1) \rightarrow (\mathbb{F}_q)^{sr} \rightarrow H^0(\mathbf{P}E, \Upsilon)^* \rightarrow 0,$$

we had to choose  $r$  points in each fiber, spanning it. As in §3, the last sequence defines a parity check matrix via evaluation of the dual points in each fiber.

An easier approach for our purposes would of course have been to start with  $T_1$  and its complete linear system  $\Upsilon_1$  in the first place, and define a code  $C$  by a parity check matrix obtained from evaluation of sections of  $\Upsilon_1$  in some more arbitrarily chosen points on the fibers of  $T_1$ . As an extreme case we could have picked all  $\mathbb{F}_q$ -rational points of all fibers. Everything said above about Step 1 of the last section would then have been unaltered, but in Step 2 we would be far from having unique decoding, unless we knew for some reason that at most a single error could be made in each individual fiber. (As mentioned in Remark 3.3, the minimum distance would be 3 in this extreme case).

Nevertheless, if one defines codes from scrolls via parity check matrices instead of via generator matrices (as evaluation codes), then one obtains a larger class of codes, for which one can interpret decoding as described above via vector bundle manipulations.

#### REFERENCES

- [BC] T. Bouganis and D. Coles, *A Geometric View of Decoding AG Codes*, Proc. AAECC-15. May, 2003.
- [Co1] D. Coles, *Vector Bundles and Codes on the Hermitian Curve*, IEEE Transactions on Information Theory, **51**, no. 6. June, 2005.
- [Co2] D. Coles, *On Constructing AG Codes without Basis Functions for Riemann-Roch Spaces*, Proc. AAECC-16. February, 2006.
- [H] R. Hartshorne, *Algebraic Geometry*, Graduate Text in Mathematics **52**, Springer Verlag (1977).
- [Ha] S.H.. Hansen, *Error-Correcting Codes from Higher-Dimensional Varieties*, Finite Fields and their applications, **7**, 530-552 (2001).
- [Hi] G. Hitching, *Geometry of vector bundle extensions and applications to the generalised theta divisor*, math.AG **0610970**, (2006).
- [J] T. Johnsen, *Rank two bundles on algebraic curves and decoding of Goppa Codes*, International Journal of Pure and Applied Mathematics, **4**, No. 1, 33-45 (2003). See also alg-geom **9608018**.
- [K] G. Kempf, *Abelian integrals*, Monografias del Instituto de Matemáticas 13. Universidad Nacional Autónoma de México, Mexico, 1983.
- [L] D. Laksov, A. Thorup, *Weierstrass points on schemes*, Journal reine und angewandte Mathematik **460** (1995), 127–164.
- [L] C.C. Lomont, *Error-correcting Codes on Algebraic Surfaces*, math.NT **0309123**, (2003).
- [Na] T. Nakashima, *Error-correcting codes on projective bundles*, Finite Fields and their applications, **12**, 222-231 (2006).
- [NR] M.S. Narasimhan, S. Ramanan, *Moduli of vector bundles on a Compact Riemann Surface*, The Annals of Mathematics, Ser. 1, **89** (1),14-51 (1969).
- [Sc] F. O. Schreyer, *Syzygies of canonical curves and special linear series*, Math. Ann. **275**, 105-137 (1986).

INST. OF ALGEBRAIC GEOMETRY, LEIBNIZ UNIVERSITY, HANNOVER, WELFENGARTEN 1, 30167 HANNOVER, GERMANY, AND, DEPT. OF MATHEMATICS, UNIVERSITY OF BERGEN, JOHS. BRUNSGT 12, N-5008 BERGEN, NORWAY

*E-mail address:* hitching@math.uni-hannover.de and johnsen@math.uib.no